

**APPLICATION FOR UNITED STATES LETTERS PATENT**

by

**SAMUEL N. ZELLNER  
MARK J. ENZMANN  
and  
ROBERT T. MOTON**

for

**SYSTEM AND METHOD FOR CONTROLLING DEVICES AT A LOCATION**

Shaw Pittman  
2300 N Street, N.W.  
Washington, D.C. 20037-1128  
(202) 663-8000

Attorney Docket No.: BS00-027  
967726/967727

## SYSTEM AND METHOD FOR CONTROLLING DEVICES AT A LOCATION

### BACKGROUND

#### Field of the Invention

5 The present invention relates to telecommunication systems, and in particular, to a system and method for controlling devices at a location.

#### Background of the Invention

Emergency telephone services are implemented throughout the world to receive calls that report emergency situations. In the United States, when a caller dials 911, the emergency call is routed to a public safety answering point (PSAP), which dispatches emergency response professionals. The emergency response professionals may include police officers, fire fighters, and paramedics. The PSAP receives from the caller critical information such as the location of the emergency, the type of emergency, and whether anyone is in imminent danger.

15 Figure 1 is a schematic diagram showing a prior art system architecture of a 911 service in the United States. The 911 service is initiated when a caller at location 100 uses telephone 102 associated with telephone line 104 to dial the number string "911." The emergency call or the 911 call is automatically routed by public switched telephone network (PSTN) 106 to PSAP 108, which is usually 20 operated by police, fire, or other emergency response professionals. The communication between the caller and PSAP 108 is a POTS (plain old telephone service) voice session.

Unlike regular telephone connections between a caller and a called party in which both parties have control over the connection, control of a 911 call rests exclusively with the called party, in this case PSAP 108. The caller of a 911 call, after establishing the POTS session, cannot terminate the session. That is, once the 5 call is connected, only PSAP 108 could end the call, usually after the emergency has been adequately resolved. This unique feature of 911 calls is necessary to ensure that the POTS session remains intact, even if the caller accidentally hangs up telephone 102, but picks up telephone 102 again at a later time, until the emergency is resolved.

10 Another feature of emergency telephone services is the capability of identifying the caller's location, i.e., location 100. For wireline telephones, the telephone service provider or PSAP 108 can maintain a 911 database, e.g., database 110, cataloging the street address for every telephone line in the area for which PSAP 108 is responsible. Referring to Figure 1, when a 911 call is made using 15 telephone 102, the street address at which the 911 call originated, i.e., the street address of location 100, can be retrieved from database 110 based on the calling party number ("CgPN") of telephone line 104 that was used to initiate the call. In other words, the telephone number of telephone line 104 is related to the street address of location 100 in database 110. Database 110 may be hereinafter referred 20 to as the 911 database. For 911 calls initiated by wireless telephones, several means for determining the calling party's location are being implemented in

accordance with the Federal Communications Commission (FCC)'s Enhanced 911 (E911) mandate.

The emergency telephone services known in the art today are limited to voice communications such as the POTS session described above. In the future, however, 5 multimedia communication sessions, including data sessions, will be more prevalent. Multimedia communication sessions could be established using, for example, integrated voice, data and video services such as those available with digital subscriber line (DSL), broadband integrated services digital networks (B-ISDN), and the like. A person could have an internal computer system within his or 10 her "multimedia capable" home. The internal computer system may be a local area network (LAN) having a number of component systems. The internal computer system can communicate with outside entities. The communication between the internal computer system and the outside entities may be via an external computer network. The external computer network may be, for example, the Internet.

15 Although the internal computer system can communicate with the outside entities using PSTN 106, the internal computer system may not be fully integrated with PSTN 106. That is, if a caller places a 911 call using the internal computer system over the voice-over-Internet protocol (VoIP), even though PSAP 108 can communicate with the caller, it cannot control the call, i.e., PSAP 108 does not have 20 exclusive control over the VoIP communication session. As a result, the caller's communication with PSAP 108 could be disconnected prematurely before PSAP 108 could adequately assess the emergency situation. Thus, a vital capability of

emergency telephone services is not available for the subscriber when he calls PSAP 108 using a non-POTS technology.

Figure 2 is a schematic diagram showing a prior art system architecture of a private security system. Location 200 may be a private residence or a commercial 5 building. Location 200 has telephone 202 that is associated with telephone line 204. Location 200 is equipped with security system 212, which may be more commonly known as the burglary alarm system.

Security system 212 may include, for example, one or more sensing apparatus such as a motion detector or glass-break sensor. When one sensing 10 apparatus is triggered, security system 212 can use telephone line 204 to contact private security firm 214 via PSTN 106. Private security firm 214 would then attempt to verify whether the triggering event warrants a dispatch of emergency 15 response professionals. For example, private security firm 214 might call someone associated with location 200 to determine whether the triggering event was a false alarm, a minor accident for which no emergency response team is needed, or another non-life-threatening incident.

If private security firm 214 cannot verify that the triggering event is not a non-life-threatening incident, private security firm 212 calls PSAP 108 to report the emergency. More often than not, however, the call to PSAP 108 is unnecessary. For 20 example, one of the sensing apparatus might have been triggered accidentally. For example, it is known that loud thunder could cause a glass-break sensor to go off,

thereby dispatching the police to location 200 unnecessarily, and resulting in wasted resources.

Technologies associated with the existing 911 service and private security system, as they exist today, are adequate to receive calls that report emergency 5 situations. These existing technologies, however, have a number of shortcomings. First, as discussed above, the existing technologies do not give VoIP emergency calls the same level of protection as calls received from POTS callers. Second, PSAP 108 does not have means for assessing, monitoring, resolving, or otherwise handling an emergency situation other than receiving second-hand information about the 10 emergency situation from the caller. Third, emergency response personnel and equipment are often dispatched to the emergency scene without knowing what emergency response equipment or personnel are required. Fourth, valuable resources are often wasted when emergency response personnel and equipment are dispatched to situations that could have been resolved without the dispatch. Fifth, 15 private security firms cannot adequately prescreen or verify reported emergency situations before dispatching the police or other emergency response team to the scene.

## SUMMARY OF THE INVENTION

20 The present invention is a system and method for controlling one or more devices associated with a location by an outside entity. The outside entity may be an emergency response unit, a private security firm, or a healthcare provider as

described in specific embodiments discussed below. The location may be a premises, a vehicle, or a person. Examples of the one or more devices can include a camera, a sprinkler system, or even a pacemaker surgically placed on a person. The system architecture of one embodiment of the present invention comprises an internal 5 computer system through which the device may be remotely controlled. The internal computer system may be a LAN. The internal computer system may also be a Bluetooth-enabled system.

When the outside entity is requested to control the device, a multimedia communication session between the internal computer system and the outside entity is established through an external computer network. The external computer network is preferably the Internet. The request for the outside entity may be made by a caller associated with the location using one of several methods, including through POTS and VoIP telephone calls. The communication session between the internal computer system and the external computer network can use one of several 10 communications protocols. Suitable communication protocols include the digital communications protocol (DCP) and the transmission control protocol (TCP). 15

In a preferred embodiment, the internal computer system is protected by a firewall. The firewall allows the outside entity to access the internal computer system to control the device if the outside entity can provide proper identity 20 information. The identity information of the outside entity may be a password that is recognized by the firewall. In the preferred embodiment, the identity information is a digital certificate issued to the outside entity by a certificate authority. The

digital certificate can be authenticated by the certificate authority before the outside entity is allowed to access the internal computer system.

When a secured tunnel through the firewall is created to enable the outside entity to access the internal computer system, the outside entity can control the 5 device that is associated with the internal computer system. The outside entity can use the device to observe a situation at the location. The outside entity can also use the device to resolve the situation, as appropriate. When the situation is resolved, the communication session between the internal computer system and the external computer network is terminated.

10 In a preferred embodiment, the outside entity has exclusive control over the communication session after the communication session is established. In other words, only the outside entity can terminate the communication session. The exclusive control allows the outside entity to resolve the situation without interruption of the communication session by other parties, including the internal 15 computer system.

In a preferred embodiment, each of the internal computer system and the outside entity is issued a digital certificate by a certificate authority. Before the secured tunnel through the firewall is created, the certificate authority must authenticate the digital certificates. This process ensures that the internal 20 computer system and the outside entity are communicating with known parties.

More importantly, this process can help protect privacy. In an embodiment in which the present invention is used to provide healthcare services, this

authentication process can ensure that medical treatment is not provided to a wrong patient.

Accordingly, it is an object of the present invention to provide a secured method for an outside entity to remotely control devices at a location.

5 It is another object of the present invention to enable an outside entity to resolve a situation at a location before dispatching emergency response professionals to the location.

10 It is another object of the present invention to enable an emergency response unit to fully observe an emergency situation before dispatching emergency response professionals to the location.

These and other objects of the present invention are described in greater detail in the detailed description of the invention, the appended drawings, and the attached claims.

## **BRIEF DESCRIPTION OF THE DRAWINGS**

Figure 1 is a schematic diagram showing a prior art system architecture of a 911 service in the United States.

Figure 2 is a schematic diagram showing a prior art system architecture of a private security system.

20 Figure 3 is a schematic diagram showing a general system architecture of an embodiment of the present invention.

Figure 4 is a schematic diagram illustrating the system architecture of a first preferred embodiment of the present invention.

Figure 5 is a flowchart illustrating the steps involved in using the first preferred embodiment of the present invention.

5 Figure 6 is a schematic diagram showing the system architecture of a second preferred embodiment of the present invention.

Figure 7 is a flowchart illustrating the steps involved in using the second preferred embodiment of the present invention.

10 Figure 8 is a schematic diagram showing the system architecture of a third preferred embodiment of the present invention.

Figure 9 is a flowchart illustrating the steps involved in using the third preferred embodiment of the present invention.

## DETAILED DESCRIPTION OF THE INVENTION

15 Figure 3 is a schematic diagram showing a general system architecture of an embodiment of the present invention. Location 300 may be any location at which internal computer system 310 may be equipped to control, operate, supervise or otherwise manipulate a number of component systems. Location 300 may be, for example, a home, an office building, or a moving object such as a yacht or an  
20 automobile.

The component systems associated with internal computer system 310 may include sensing apparatus 314, observation device 316, and emergency response

device 318. Sensing apparatus 314 may be one of several motion detectors commonly available in the market. Observation device 316 may be a commonly available video camera or a more sophisticated surveillance camera. Emergency response device 318 may be a sprinkler system that can be activated by internal 5 computer system 310. Other component systems that can be associated with internal computer system 310 can include heating, ventilation, and air conditioning systems, telephone systems, etc.

Through internal computer system 310, each of the component systems at 10 location 300 is networked to each other so that the component systems can work together. For example, a first action by a first component system can activate a second component system to perform a second action through internal computer system 310. Internal computer system 310 may be a single computer. Internal computer system 310 may also be a LAN.

Firewall 340 can protect internal computer system 310 from unauthorized 15 access by external entities. For example, firewall 340 can protect internal computer system 310 from undesirable access by outside entity 390 via communication links 392 and 342. Communication link 342 may be a telephone line, a DSL, a T1 line, a T3 line, a B-ISDN line, and the like. Firewall 340 can allow a user of internal computer system 310 to access external computer network 370, while also 20 preventing crackers, hackers or others on external computer network 370 from accessing internal computer system 310. External computer network 370 may be, for example, the Internet.

Firewall 340 can comprise a combination of hardware and software that is built using routers, servers, and a variety of software. Firewall 340 can be simple or complex, depending on the desired levels of security. Firewall 340 can have a number of elements including, for example: (1) an internal screening router

5 (sometimes called a choker router) used to provide packet filtering; (2) a bastion host or a proxy server used as a go-between to maintain security and log all traffic between internal computer system 310 and external computer network 370; and (3) an exterior screening router used to provide an extra level of protection if the internal screening router fails.

10 Telephone 302 is an example of customer premises equipment (CPE) that can use telephone line 304 to make POTS calls via PSTN 106 to outside entities, including outside entity 390. Outside entity 390 may be an emergency response unit such as PSAP 108 of Figures 1 and 2. Outside entity 390 may also be a private security firm, such as private security firm 214 of Figure 2. Wireless device 322 can also contact outside entity 390. For example, wireless device 322 may be a wireless telephone that can communicate with outside entity 390 using wireless communication link 323 through base station 324 and mobile telephone switching office (MTSO) 326.

15

Database 380 is accessible by outside entity 390. Database 380 can contain

20 information that is typically found in a 911 database, such as database 110 shown in Figure 1 and as described in the background section above. For example, database 380 can contain, among other information, the street address of location

300. In addition, database 380 may also comprise other information such as a profile of location 300, including without limitation, the Internet Protocol (IP) address of internal computer system 310. Furthermore, database 380 may comprise additional information related to each of the component systems. Database 380 also 5 preferably has information related to the physical layout of each of the component systems at location 300, and instructions for operating them remotely. More importantly, database 380 may also comprise medical profiles of residents of location 300.

10 In addition, database 380 can contain additional information related to how outside entity 390 may be authorized to access internal computer system 310. Specifically, database 380 can comprise information related to how outside entity 390 may establish a secured tunnel through firewall 340 on communication link 342. For example, database 380 can contain identity information of outside entity 390. The identity information may be a password, an access code, or a key. The 15 identity information is preferably issued to outside entity 390 by internal computer system 310. The identity information can also be a digital certificate issued by certificate authority 360. The identity information can be used by outside entity 390 to go through firewall 340 to access internal computer system 310. Preferably, database 380 can be enhanced with information related to public key infrastructure 20 (PKI). The PKI can have the following capabilities:

1. Authenticate identity. Digital certificates issued as part of the PKI can allow individual users, organizations, and website operators to

confidentially validate the identity of each party in an Internet transaction.

2. Verify integrity. A digital certificate can ensure that the message or document that the certificate "signs" has not been changed or corrupted in transit online.
3. Ensure privacy. The digital certificates can protect information from interception during Internet transmission.
4. Authorize access. The digital certificates can replace easily guessed and frequently lost user IDs and passwords to streamline intranet login security and they can reduce management information system (MIS) overhead.
5. Authorize transactions. With PKI solutions, an enterprise can control access privileges for specified online transactions.
6. Support for nonrepudiation. The digital certificates can validate their users' identities, making it nearly impossible to later repudiate a digitally "signed" transaction, such as a purchase made on a website.

The digital certificates associated with the PKI can be issued and/or authenticated by certificate authority 360. To get a digital certificate, outside entity 390 and/or internal computer system 310 can visit certificate authority 360, preferably, via external computer network 370 on communication link 362, and request the certificate. The user's name and other identifying information are typically required to obtain the digital certificate. The digital certificate can be

digitally signed to guarantee its authenticity. The digital certificate is unique to the user and it can be put on a memory (e.g., hard disk) of a computer, along with a private key. The digital certificate can comprise the name of the user, the name of certificate authority 360, the unique serial number of the certificate, the version number of the certificate, the expiration date of the certificate, the user's public key, and the digital signature of certificate authority 360. The exact format of the digital certificate can be defined by a standard. The standard may be the well-known 5 X.509 standard.

10 A communication session between internal computer system 310 and outside entity 390 may be established via external computer network 370, along communication link 342 and 392. The communication session can be a multimedia session that uses one of several communications protocols. For example, Digital Communications Protocol (DCP) or Transmission Control Protocol (TCP) may be used in conjunction with Internet Protocol (IP). Using the PKI described above, the 15 communication session between internal computer system 310 and outside entity 390 can be established as a secured tunnel through firewall 340.

One or both of internal computer system 310 and outside entity 390 can 20 initiate the creation of the secured tunnel. Furthermore, the secured tunnel can be created as a result of the establishment of a POTS or VoIP session initiated by a caller associated with location 300. For example, the system of the present invention can be adapted such that when the telephone number of outside entity 390 is dialed on telephone 302 or wireless device 322, the dialing of the telephone

number can serve as an instruction for internal computer system 310 to establish the communication session with outside entity 390. Similarly, outside entity 390 can initiate the communication session, via communication link 342, with internal computer system 310 when outside entity 390 is contacted by the caller associated 5 with location 300. Outside entity 390 can retrieve information related to location 300, e.g., the IP address of internal computer system 310, from database 380. During the communication session, outside entity 390 can control one or more of the component systems (including sensing apparatus 314, observation device 316, and emergency response device 318). The scope of the control can be regulated by 10 firewall 340.

15 In preferred embodiments of the present invention, control of the communication session after the communication session is established, can rest exclusively with outside entity 390. In other words, once the communication session is established between internal computer system 310 and outside entity 390, only outside entity 390 can terminate the communication session.

16 In light of the above disclosure, it is clear that a large number of 20 embodiments may be implemented for the present invention. For the purposes of demonstration, three specific examples of how the present invention may be implemented are discussed below. Although the following examples best illustrate the present invention, one of ordinary skill in the art would appreciate that other embodiments are possible in light of the disclosure. In addition, while the system operation described herein and illustrated in the diagrams and flowcharts contains

many specific details, these specific details should not be construed as limitations on the scope of the invention, but rather as examples of how preferred embodiments of the invention may be implemented. As would be apparent to one of ordinary skill in the art, many other variations on the system operation are possible, including 5 differently grouped and ordered method steps. Accordingly, the scope of the invention should be determined not by the embodiments illustrated, but by the appended claims and their equivalents.

Figure 4 is a schematic diagram illustrating the system architecture of a first preferred embodiment of the present invention. Location 400 may be a residential unit, an office building, a boat, an automobile, or any location at which a LAN may be set up. LAN 410 can be similar to internal computer system 310 described above for Figure 3. LAN 410 can comprise LAN server 430, which can control, operate, supervise, and otherwise manipulate all component systems that are associated with LAN 410. The component systems may include, for example, computer system 421, video system 422, audio system 423, climate control system 424, fire alarm system 425, security system 426, electrical system 427, and telephone system 428. 10 15

Computer system 421 may comprise one or more desktop computers, mainframe computers, laptop computers, and any other peripherals including, without limitation, printers, scanners, cameras, microphones, and speakers. Video system 422 may include cameras, television sets, and video cassette recorders. 20 Examples of audio system 423 may be stereos, compact disk players, and intercoms. Climate control system 424 may include heating, ventilation, and air conditioning

units installed at location 400, and the associated sensors, thermostats, and water heaters. Fire alarm system 425 may comprise, for example, fire alarm units and sprinkler systems. Security system 426 may include, among other things, motion detectors, surveillance cameras, glass-break sensors, as well as others sensors 5 normally included as part of a security system. Electrical system 427 can operate all electrical equipment and appliances that are installed at location 400 including microwaves, baby monitors, refrigerators, photocopying machines, and vacuums.

Telephone system 428 includes all CPE that can communicate with PSTN 106 including wireline telephones, wireless telephones, and facsimile machines.

10 Through LAN server 430, each of the component systems associated with LAN 410 can communicate and share resources with other component systems. For example, video system 422 and security system 426 may share common cameras on their systems. In addition, security system 426 and telephone system 428 may work together to report or record a suspicious activity observed at location 400 via 15 PSTN 106. Furthermore, electrical system 427 and computer system 421 may work together to communicate with external computer network 370 so that an appliance on electrical system 427 may be controlled remotely by the owner of location 400 via external computer network 370. LAN server 430 may also manipulate other systems not shown in Figure 4 so long as the other systems are part of LAN 410 and 20 connected to LAN server 430.

LAN server 430 can be protected by firewall 440 to prevent unauthorized access by external entities via communication link 442. Communication link 442

can be a DSL, a T1 line, a T3 link, a B-ISDN line and the like. Firewall 440 may comprise one or more elements as described above for firewall 340 of Figure 3. To go through firewall 440, an outside entity such as emergency response unit 490 can be required to provide identity information. The identity information can be a key, 5 an access code, or a password. Emergency response unit 490 may be a PSAP. The identity information can be issued to emergency response entity 490 by LAN server 430.

Preferably, identity information comprising a properly authenticated digital certificate is required before any external entity is allowed to communicate with 10 LAN server 430. For example, emergency response unit 490 must supply its digital certificate authenticated by certification authority 360 before it can communicate with LAN server 430. A secured tunnel through firewall 440 may be established after certificate authority 360 authenticates the digital certificate of emergency 15 response unit 490. Similarly, emergency response unit 490 may require LAN server 430 to supply the latter's digital certificate before emergency response unit 490 would operate any of the component systems associated with LAN 410. Emergency response entity 490 can communicate with LAN server 430 via external computer network 370 on communication links 497 and 442. Certificate authority 360 can be contacted via external computer network 370 using communication link 362.

20 Database 480 can be similar to database 380 of Figure 3. In this embodiment, information related to LAN 410 can be supplied by the owner of LAN 410 to database 480 using any one of several methods. For example, the

information may be supplied through a POTS session by the owner using telephone system 428 via PSTN 106 on communication links 402 and 476. Similarly, the information related to LAN 410 may be supplied by the owner through a VoIP session by computer system 421 via external computer network 370 on communication links 472 and 478. The information related to LAN 410 can be retrieved by emergency response unit 490 using communication link 498.

Emergency response entity 490 can communicate with external computer network 370 and PSTN 106 using communication links 497 and 492, respectively. The communication on any of communication links 442, 362, 478, 497, and 498 may use any suitable communications protocol. For example, one of DCP and TCP may be used.

The system of the present invention can be adapted such that when emergency response unit 490 is contacted by the owner using one or both of computer system 421 and telephone system 428, either LAN server 430 or emergency response unit 490 can initiate a communication session using communication link 442 via external computer network 370. In other words, the very act of the owner of LAN 410 contacting emergency response unit 490 can give emergency response unit 490 the permission to control one or more component systems associated with LAN 410. Firewall 440 can be adapted so that emergency response unit 490 can have control over LAN 410 through a secured tunnel.

Firewall 440 can also be adapted to provide emergency response unit 490 different levels of access or security. In one example, emergency response unit 490 may have

control over one system component of LAN 410. In an extreme example, emergency response unit 490 may have exclusive, unhindered, total control over all component systems of LAN 410.

Figure 5 is a flowchart illustrating the steps involved in using the first 5 preferred embodiment of the present invention. In step 502, LAN 410 can be set up at location 400 as described above. For example, LAN 410 can comprise LAN server 430 that is in communication with various component systems associated with LAN 410, including computer system 421, video system 422, audio system 423, climate control system 424, fire alarm system 425, security system 426, electrical system 427, and telephone system 428. A component or device of each of these component 10 systems may function as one or more of sensing apparatus, observation devices, and emergency response devices. A sensing apparatus can cause LAN server 410 to contact emergency response unit 490 when the sensing apparatus detects a triggering event. When the contact is made, LAN 410 can request emergency 15 response unit 490 to control one or more devices associated with LAN 410. An observation device can allow emergency response unit 490 to observe and monitor a situation at location 400. An emergency response device can allow emergency response unit 490 to resolve the situation at location 400. Each of the sensing 20 apparatus, observation devices, and the emergency response devices can have overlapping functions.

In step 504, firewall 440 can be built to protect LAN 410. As described above, firewall 440 can have one or more elements. Firewall 440 can have different

levels of security. Also in step 504, database 480 associated with emergency response unit 490 can be populated with information. The information may be that which is available to database 380 as described above. In addition, the information may include information related to LAN 410 and its component systems, including

- 5 the IP address of LAN server 430. Population of database 480 may be performed using one of several methods. For example, the information can be provided to database 480 by using computer system 421 via external computer network 370.

Similarly, the information can be supplied using telephone system 428 via PSTN

106. Identity information such as a password to go through firewall 440 may be provided to database.

In step 506, the owner of LAN 410 can decide on how emergency response unit 490 can be authorized to access LAN 410 through a secured tunnel in firewall 440. For example, it could be decided that emergency response unit 490 must supply a password or a digital certificate authenticated by certificate authority 360 before access to LAN 410 is granted. Furthermore, it may be agreed upon that emergency response unit 490 will not be allowed to access LAN 410 unless one of the component systems associated with LAN 410 has contacted emergency response unit 490 first.

In step 508, a triggering event is detected at location 400. The triggering 20 event may be a suspicious movement detected by one of the component systems associated with LAN 410. In step 510, the triggering event can be reported to emergency response unit 490 using one of several methods. For example, a

telephone that is associated with telephone system 428 can be used to contact emergency response unit 490 through PSTN 106 in a POTS session. Similarly, the triggering event can be reported to emergency response unit 490 using a computer that is associated with computer system 421 through external computer network 5 370 in a VoIP session. Furthermore, a wireless telephone associated with telephone system 428 can be used to contact emergency response unit 490. In the preferred embodiment, LAN server 430 can be notified that emergency response entity 490 has been contacted about the triggering event.

10 In step 512, when emergency response unit 490 receives the report about the triggering event at location 400, emergency response unit 490 can consult database 480 to retrieve information associated with location 400. The information may comprise the password to access LAN 410, IP address of LAN server 430, and information related to the various component systems of LAN 410.

15 In step 514, emergency response unit 490 can initiate a communication session with LAN 410. The communication session can be initiated because emergency response unit 490 has the IP address of LAN server 430. In step 516, at 20 firewall 440, emergency response unit 490 can be required to provide a proper form of authority. For example, emergency response unit 490 may be required to provide the password. Alternatively, emergency response unit 490 may be required to supply a digital certificate authenticated by certificate authority 360, before it can access LAN 410.

In step 518, when the identity of emergency response unit 490 is properly ascertained by firewall 440, either by using the password or the digital certificate, a secured tunnel through firewall 440 can be created. A communication session between emergency response unit 490 and LAN server 430 can be established using 5 one of several communications protocols, including DCP and TCP. Preferably, emergency response unit 490 has exclusive control over the communication session.

In step 520, emergency response unit 490 can observe the situation at location 400. Using information retrieved from database 480, emergency response unit 490 can know which component system or systems associated with LAN 410 10 can be used as an observation device to monitor the situation.

Similarly, in step 522, emergency response unit 490 may use one or more of the component systems associated with LAN 410 as emergency response devices to resolve the situation. For example, if it was observed that a suspicious person is moving about within location 400, emergency response unit 490 may use a camera 15 to identify the person. Furthermore, emergency response unit 490 may use a loudspeaker controlled by LAN server 430 to ask the person to leave location 400 immediately. Of course, emergency response unit 490 can also dispatch police officers to location 400, if warranted.

In step 524, the communication session can be terminated when the 20 emergency situation is resolved. As mentioned above, preferably only emergency response unit 490 can terminate the communication session. The secured tunnel is shut as soon as the communication session is terminated, ending emergency

response unit 490's access to LAN 410. LAN server 430 preferably has a display that can indicate whether the communication session is still active. If a second triggering event is detected, emergency response unit 490 must go through at least steps 514 and 516 before it can communicate with LAN 410 again.

5       Figure 6 is a schematic diagram showing the system architecture of a second preferred embodiment of the present invention. In this embodiment, location 600 may be an office building of a business entity, a residence, a yacht, an automobile, or any location at which an internal computer system associated with at least one component system or device may be set up. CPE 602, telephone line 604, internal computer system 610, firewall 640, communication link 642, sensing apparatus 614, observation device 616, and emergency response device 618 are similar to corresponding elements shown in Figure 3 and described above.

10       Sensing apparatus 614 can be used to detect a triggering event at location 600. Observation device 616 can be used to observe the situation associated with the triggering event at location 600. Emergency response device 618 can be used to resolve the situation. Each of sensing apparatus 614, observation device 616, and emergency response device 618 may be selected from the various components of video system 422, audio system 423, climate control system 424, fire alarm system 425, security system 426, and electrical system 427 as described above and shown in  
15       Figure 4. For example, sensing apparatus 614 may be a thermostat associated with climate control system 424; observation device 616 may be a video camera  
20

associated with video system 422; and emergency response device 618 may be a sprinkler system associated with fire alarm system 425.

Internal computer system 610 is in communication with CPE 602, sensing apparatus 614, observation device 616, and emergency response device 618.

- 5 Internal computer system 610 is protected by firewall 640, which can be similar to firewalls 340 and 440 described above.

When sensing apparatus 614 detects the triggering event, e.g., the temperature at location 600 has risen above a certain threshold, internal computer system 610 can report the triggering event to private security firm 614. The report to private security firm 614 can be made using telephone line 604 via PSTN 106. 10 Internal computer system 610 may be adapted to initiate a communication session with private security firm 614 via external computer network 370 along communication links 642 and 692 when private security firm 614 is contacted using telephone line 604. Through the communication session, private security firm 614 can control one or more devices associated with internal computer system 610. 15

Private security firm 614 preferably has exclusive control over the communication session. Private security firm 614 preferably can retrieve information related to the devices from database 680. Private security firm 614 can also communicate with PSAP 108 that has access to database 110.

- 20 Figure 7 is a flowchart illustrating the steps involved in using the second preferred embodiment of the present invention. In step 702, a triggering event is detected by sensing apparatus 614. The triggering event may be, for example, a

temperature higher than a threshold that is associated with location 600. The triggering event could also be noise of a certain intensity, or a motion at a certain time of day.

5 In step 704, private security firm 614 is contacted to report the triggering event. The contact may be made manually, e.g., by a person dialing the telephone number of private security firm 614 using CPE 602. Preferably, the contact may also be made using a computer associated with internal computer system 610.

10 Furthermore, private security firm 614 may be contacted using an e-mail. Private security firm 614 may have an IP address to which a report about the triggering event may be sent by internal computer system 610. In one embodiment, step 704 may not be a necessary step.

15 In step 706, a communication session between internal computer system 610 and private security firm 614 can be established. Internal computer system 610 can place a QoS (quality of service) priority call to private security firm 614. The establishment of the communication session may be accomplished through communication links 642 and 692 via external computer network 370. Internal computer system 610 and private security firm 614 can exchange digital certificates during the communication session. The identity of the parties can be authenticated by certificate authority 360 in step 708.

20 In step 710, after the parties have ascertained the identities of each other through the authentication process, private security firm 614 can observe the situation at location 600 using observation device 616. During the communication

session, private security firm 614 may use the information in database 680 to operate observation device 616 to monitor the situation at location 600. For example, private security firm 614 may observe, through a camera, that a first person had fainted in the kitchen. Private security firm 614 may also observe that

5 a second person is watching a movie in a bedroom, unaware of the first person's condition.

In step 712, private security firm 614 can evaluate whether it can resolve the situation on its own. If so, in step 714, private security firm 614 may resolve the situation using emergency response device 618. For example, private security firm 10 614 may use emergency response device 618, e.g., an intercom, through which private security firm 614 may alert the second person in the bedroom that the first person had fainted in the kitchen. Alternatively, private security firm 614 may use a different emergency response device, e.g., a sprinkler in the kitchen, to wake up the first person. The method can be modified so that if the situation cannot be 15 successfully resolved in step 714, the process can go to step 718. The communication session may be terminated in step 716 by private security firm 614 after the situation at location 600 has been resolved, e.g., the first person has been awaken successfully and is observed to be in good health.

If, in step 712, private security firm 614 determined that it could not resolve 20 the situation on its own, the process goes to step 718 in which a third party may be contacted by private security firm 614. The third party may be an emergency

response unit, such as emergency response unit 490 described above. In step 720, the communication session can be transferred to the third party.

Figure 8 is a schematic diagram showing the system architecture of a third preferred embodiment of the present invention. In the third preferred embodiment, 5 the present invention can be adapted to operate on Bluetooth-enabled devices and technologies. Information related to Bluetooth technology can be found in Bluetooth Protocol Architecture, Version 1.0 (August 25, 1999), which is hereby incorporated by reference in its entirety.

10 Patient 800 can be a person with a health condition that requires constant medical monitoring. Patient 800's pulse, blood pressure, blood oxygen saturation level, body temperature etc., may be taken or measured by vital sign monitor 814, which is preferably worn by patient 800 at all times. Vital sign monitor 814 can be adapted to communicate with healthcare computer 810. Healthcare computer 810 is preferably a small, portable computer that is Bluetooth compatible. Firewall 840 15 can be created using a combination of hardware and software as described above. Firewall 840 can be integrated as part of healthcare computer 810. Firewall 840 protects healthcare computer 810 from unauthorized access by others. A digital certificate issued to healthcare computer 810 can be stored in a memory of healthcare computer 810.

20 In addition to vital sign monitor 814, healthcare computer 810 can be associated with other component systems, including video camera 816 and pacemaker 818. Video camera 816 may be installed at a location where patient 800

normally spends most of his or her time. For example, video camera 816 may be installed in the bedroom of patient 800. Pacemaker 818, as known to one skilled in the art, can be surgically placed within the body of patient 800. Vital sign monitor 814, video camera 816, and pacemaker 818 are also preferably Bluetooth-enabled.

5 When vital sign monitor 814 detects a triggering event, vital sign monitor 814 can report the triggering event to healthcare computer 810. The triggering event may occur, for example, when the pulse of patient 800 drops below a certain threshold or when the body temperature rises above a certain limit. Healthcare computer 810, in turn, can communicate with healthcare provider 890 using wireless device 822. Wireless device 822 can be adapted to contact healthcare provider 890 when the triggering event is detected. Wireless device 822 may be a specialty item that can be designed or dedicated to notify healthcare provider 890 of patient 800's conditions. In another embodiment, wireless device 822 is preferably Bluetooth-enabled and can communicate with healthcare computer 810. In another embodiment, a person who observes that patient 800 requires help may contact healthcare provider 890 using wireless device 822, which can be a regular wireless telephone. Wireless device 822 can communicate with healthcare provider 890 through communication link 823, base station 324, MTSO 326, and PSTN 106.

10 Healthcare provider 890 preferably has information related to patient 800.

15 The information is preferably stored in database 880, which is accessible by healthcare provider 890. The information may comprise the medical history of patient 800 and all information associated with healthcare computer 810, including

those related to vital sign monitor 814, video camera 816, pacemaker 818, and wireless device 822. The information may also include a digital certificate issued to healthcare provider 890 that would enable healthcare provider 890 to pass through firewall 840 during a communication session. Healthcare provider 890 can operate 5 one or more component systems associated with healthcare computer 810 through external computer network 370. Preferably, database 880 has PKI information for access to healthcare computer 880. For example, healthcare provider 890 can control pacemaker 818 during a communication session along communication links 892 and 842. Certificate authority 360, accessible using communication link 362, can provide authentication services to healthcare provider 890 and patient 800 to ensure that the communication session between healthcare provider 890 and 10 healthcare computer 810 is a secured tunnel.

15 Figure 9 is a flowchart illustrating the steps involved in using the third preferred embodiment of the present invention. In step 902, healthcare computer 810 and its associated devices can be set up as described above. In step 904, information regarding patient 800 is provided to database 880. The information can comprise the medical records of patient 800 and operating instructions of the various component systems associated with healthcare computer 810. Database 880 can also be populated with information related to how a secured tunnel through 20 firewall 840 may be established.

In step 906, when a triggering event occurs, vital sign monitor 814 can detect the triggering event. In step 908, healthcare provider 890 can be contacted using

wireless device 822. In step 910, healthcare provider 890 can consult database 880 to obtain information about patient 800. In step 912, healthcare provider 890 can initiate a communication session with healthcare computer 810 via external computer network 370.

5        In step 914, healthcare provider 890 and healthcare computer 810 can exchange their digital certificates. In step 916, the digital certificates are authenticated. Authentication of the digital certificates can be done by certificate authority 360. The authentication process ensures that healthcare provider 890 is treating the right patient and that patient 800 is treated by his or her healthcare provider.

10        If, in step 916, the digital certificates are not authenticated, the process ends and healthcare provider 890 is denied access to healthcare computer 810. But if in step 916 both digital certificates are authenticated, a communication session between healthcare provider 890 and healthcare computer 810 is established in step 15 918. The communication session is preferably a secured tunnel through firewall 840. In step 920, healthcare provider 890 can observe the condition of patient 810. The condition may be observed using one or more of vital sign monitor 814 and video camera 816. In step 922, if warranted, healthcare provider can control an emergency response device, such as pacemaker 816, to help improve the medical 20 condition of patient 800. The communication session is terminated in step 924 when healthcare provider 890 is satisfied with the condition of patient 800.

Preferably, control of the communication session rests exclusively with healthcare provider 890.

The foregoing disclosure of embodiments and specific examples of the present invention has been presented for purposes of illustration and description. It is not 5 intended to be exhaustive or to limit the invention to the precise forms disclosed.

Many variations and modifications of the embodiments described herein will be obvious to one of ordinary skill in the art in light of the above disclosure. The scope of the invention is to be defined only by the claims appended hereto, and by their equivalents.

10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36  
37  
38  
39  
40  
41  
42  
43  
44  
45  
46  
47  
48  
49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59  
60  
61  
62  
63  
64  
65  
66  
67  
68  
69  
70  
71  
72  
73  
74  
75  
76  
77  
78  
79  
80  
81  
82  
83  
84  
85  
86  
87  
88  
89  
90  
91  
92  
93  
94  
95  
96  
97  
98  
99  
100  
101  
102  
103  
104  
105  
106  
107  
108  
109  
110  
111  
112  
113  
114  
115  
116  
117  
118  
119  
120  
121  
122  
123  
124  
125  
126  
127  
128  
129  
130  
131  
132  
133  
134  
135  
136  
137  
138  
139  
140  
141  
142  
143  
144  
145  
146  
147  
148  
149  
150  
151  
152  
153  
154  
155  
156  
157  
158  
159  
160  
161  
162  
163  
164  
165  
166  
167  
168  
169  
170  
171  
172  
173  
174  
175  
176  
177  
178  
179  
180  
181  
182  
183  
184  
185  
186  
187  
188  
189  
190  
191  
192  
193  
194  
195  
196  
197  
198  
199  
200  
201  
202  
203  
204  
205  
206  
207  
208  
209  
210  
211  
212  
213  
214  
215  
216  
217  
218  
219  
220  
221  
222  
223  
224  
225  
226  
227  
228  
229  
230  
231  
232  
233  
234  
235  
236  
237  
238  
239  
240  
241  
242  
243  
244  
245  
246  
247  
248  
249  
250  
251  
252  
253  
254  
255  
256  
257  
258  
259  
259  
260  
261  
262  
263  
264  
265  
266  
267  
268  
269  
269  
270  
271  
272  
273  
274  
275  
276  
277  
278  
279  
279  
280  
281  
282  
283  
284  
285  
286  
287  
288  
289  
289  
290  
291  
292  
293  
294  
295  
296  
297  
298  
299  
299  
300  
301  
302  
303  
304  
305  
306  
307  
308  
309  
309  
310  
311  
312  
313  
314  
315  
316  
317  
318  
319  
319  
320  
321  
322  
323  
324  
325  
326  
327  
328  
329  
329  
330  
331  
332  
333  
334  
335  
336  
337  
338  
339  
339  
340  
341  
342  
343  
344  
345  
346  
347  
348  
349  
349  
350  
351  
352  
353  
354  
355  
356  
357  
358  
359  
359  
360  
361  
362  
363  
364  
365  
366  
367  
368  
369  
369  
370  
371  
372  
373  
374  
375  
376  
377  
378  
379  
379  
380  
381  
382  
383  
384  
385  
386  
387  
388  
389  
389  
390  
391  
392  
393  
394  
395  
396  
397  
398  
399  
399  
400  
401  
402  
403  
404  
405  
406  
407  
408  
409  
409  
410  
411  
412  
413  
414  
415  
416  
417  
418  
419  
419  
420  
421  
422  
423  
424  
425  
426  
427  
428  
429  
429  
430  
431  
432  
433  
434  
435  
436  
437  
438  
439  
439  
440  
441  
442  
443  
444  
445  
446  
447  
448  
449  
449  
450  
451  
452  
453  
454  
455  
456  
457  
458  
459  
459  
460  
461  
462  
463  
464  
465  
466  
467  
468  
469  
469  
470  
471  
472  
473  
474  
475  
476  
477  
478  
479  
479  
480  
481  
482  
483  
484  
485  
486  
487  
488  
489  
489  
490  
491  
492  
493  
494  
495  
496  
497  
498  
499  
499  
500  
501  
502  
503  
504  
505  
506  
507  
508  
509  
509  
510  
511  
512  
513  
514  
515  
516  
517  
518  
519  
519  
520  
521  
522  
523  
524  
525  
526  
527  
528  
529  
529  
530  
531  
532  
533  
534  
535  
536  
537  
538  
539  
539  
540  
541  
542  
543  
544  
545  
546  
547  
548  
549  
549  
550  
551  
552  
553  
554  
555  
556  
557  
558  
559  
559  
560  
561  
562  
563  
564  
565  
566  
567  
568  
569  
569  
570  
571  
572  
573  
574  
575  
576  
577  
578  
579  
579  
580  
581  
582  
583  
584  
585  
586  
587  
588  
589  
589  
590  
591  
592  
593  
594  
595  
596  
597  
598  
599  
599  
600  
601  
602  
603  
604  
605  
606  
607  
608  
609  
609  
610  
611  
612  
613  
614  
615  
616  
617  
618  
619  
619  
620  
621  
622  
623  
624  
625  
626  
627  
628  
629  
629  
630  
631  
632  
633  
634  
635  
636  
637  
638  
639  
639  
640  
641  
642  
643  
644  
645  
646  
647  
648  
649  
649  
650  
651  
652  
653  
654  
655  
656  
657  
658  
659  
659  
660  
661  
662  
663  
664  
665  
666  
667  
668  
669  
669  
670  
671  
672  
673  
674  
675  
676  
677  
678  
679  
679  
680  
681  
682  
683  
684  
685  
686  
687  
688  
689  
689  
690  
691  
692  
693  
694  
695  
696  
697  
698  
698  
699  
699  
700  
701  
702  
703  
704  
705  
706  
707  
708  
709  
709  
710  
711  
712  
713  
714  
715  
716  
717  
718  
719  
719  
720  
721  
722  
723  
724  
725  
726  
727  
728  
729  
729  
730  
731  
732  
733  
734  
735  
736  
737  
738  
739  
739  
740  
741  
742  
743  
744  
745  
746  
747  
748  
749  
749  
750  
751  
752  
753  
754  
755  
756  
757  
758  
759  
759  
760  
761  
762  
763  
764  
765  
766  
767  
768  
769  
769  
770  
771  
772  
773  
774  
775  
776  
777  
778  
779  
779  
780  
781  
782  
783  
784  
785  
786  
787  
788  
789  
789  
790  
791  
792  
793  
794  
795  
796  
797  
798  
798  
799  
799  
800  
801  
802  
803  
804  
805  
806  
807  
808  
809  
809  
810  
811  
812  
813  
814  
815  
816  
817  
818  
819  
819  
820  
821  
822  
823  
824  
825  
826  
827  
828  
829  
829  
830  
831  
832  
833  
834  
835  
836  
837  
838  
839  
839  
840  
841  
842  
843  
844  
845  
846  
847  
848  
849  
849  
850  
851  
852  
853  
854  
855  
856  
857  
858  
859  
859  
860  
861  
862  
863  
864  
865  
866  
867  
868  
869  
869  
870  
871  
872  
873  
874  
875  
876  
877  
878  
879  
879  
880  
881  
882  
883  
884  
885  
886  
887  
888  
889  
889  
890  
891  
892  
893  
894  
895  
896  
897  
898  
898  
899  
899  
900  
901  
902  
903  
904  
905  
906  
907  
908  
909  
909  
910  
911  
912  
913  
914  
915  
916  
917  
918  
919  
919  
920  
921  
922  
923  
924  
925  
926  
927  
928  
929  
929  
930  
931  
932  
933  
934  
935  
936  
937  
938  
939  
939  
940  
941  
942  
943  
944  
945  
946  
947  
948  
949  
949  
950  
951  
952  
953  
954  
955  
956  
957  
958  
959  
959  
960  
961  
962  
963  
964  
965  
966  
967  
968  
969  
969  
970  
971  
972  
973  
974  
975  
976  
977  
978  
979  
979  
980  
981  
982  
983  
984  
985  
986  
987  
988  
988  
989  
989  
990  
991  
992  
993  
994  
995  
996  
997  
998  
998  
999  
999  
1000  
1001  
1002  
1003  
1004  
1005  
1006  
1007  
1008  
1009  
1009  
1010  
1011  
1012  
1013  
1014  
1015  
1016  
1017  
1018  
1019  
1019  
1020  
1021  
1022  
1023  
1024  
1025  
1026  
1027  
1028  
1029  
1029  
1030  
1031  
1032  
1033  
1034  
1035  
1036  
1037  
1038  
1039  
1039  
1040  
1041  
1042  
1043  
1044  
1045  
1046  
1047  
1048  
1049  
1049  
1050  
1051  
1052  
1053  
1054  
1055  
1056  
1057  
1058  
1059  
1059  
1060  
1061  
1062  
1063  
1064  
1065  
1066  
1067  
1068  
1069  
1069  
1070  
1071  
1072  
1073  
1074  
1075  
1076  
1077  
1078  
1079  
1079  
1080  
1081  
1082  
1083  
1084  
1085  
1086  
1087  
1088  
1088  
1089  
1089  
1090  
1091  
1092  
1093  
1094  
1095  
1096  
1097  
1098  
1098  
1099  
1099  
1100  
1101  
1102  
1103  
1104  
1105  
1106  
1107  
1108  
1109  
1109  
1110  
1111  
1112  
1113  
1114  
1115  
1116  
1117  
1118  
1119  
1119  
1120  
1121  
1122  
1123  
1124  
1125  
1126  
1127  
1128  
1129  
1129  
1130  
1131  
1132  
1133  
1134  
1135  
1136  
1137  
1138  
1139  
1139  
1140  
1141  
1142  
1143  
1144  
1145  
1146  
1147  
1148  
1149  
1149  
1150  
1151  
1152  
1153  
1154  
1155  
1156  
1157  
1158  
1159  
1159  
1160  
1161  
1162  
1163  
1164  
1165  
1166  
1167  
1168  
1169  
1169  
1170  
1171  
1172  
1173  
1174  
1175  
1176  
1177  
1178  
1179  
1179  
1180  
1181  
1182  
1183  
1184  
1185  
1186  
1187  
1188  
1188  
1189  
1189  
1190  
1191  
1192  
1193  
1194  
1195  
1196  
1197  
1198  
1198  
1199  
1199  
1200  
1201  
1202  
1203  
1204  
1205  
1206  
1207  
1208  
1209  
1209  
1210  
1211  
1212  
1213  
1214  
1215  
1216  
1217  
1218  
1219  
1219  
1220  
1221  
1222  
1223  
1224  
1225  
1226  
1227  
1228  
1229  
1229  
1230  
1231  
1232  
1233  
1234  
1235  
1236  
1237  
1238  
1239  
1239  
1240  
1241  
1242  
1243  
1244  
1245  
1246  
1247  
1248  
1249  
1249  
1250  
1251  
1252  
1253  
1254  
1255  
1256  
1257  
1258  
1259  
1259  
1260  
1261  
1262  
1263  
1264  
1265  
1266  
1267  
1268  
1269  
1269  
1270  
1271  
1272  
1273  
1274  
1275  
1276  
1277  
1278  
1279  
1279  
1280  
1281  
1282  
1283  
1284  
1285  
1286  
1287  
1288  
1288  
1289  
1289  
1290  
1291  
1292  
1293  
1294  
1295  
1296  
1297  
1298  
1298  
1299  
1299  
1300  
1301  
1302  
1303  
1304  
1305  
1306  
1307  
1308  
1309  
1309  
1310  
1311  
1312  
1313  
1314  
1315  
1316  
1317  
1318  
1319  
1319  
1320  
1321  
1322  
1323  
1324  
1325  
1326  
1327  
1328  
1329  
1329  
1330  
1331  
1332  
1333  
1334  
1335  
1336  
1337  
1338  
1339  
1339  
1340  
1341  
1342  
1343  
1344  
1345  
1346  
1347  
1348  
1349  
1349  
1350  
1351  
1352  
1353  
1354  
1355  
1356  
1357  
1358  
1359  
1359  
1360  
1361  
1362  
1363  
1364  
1365  
1366  
1367  
1368  
1369  
1369  
1370  
1371  
1372  
1373  
1374  
1375  
1376  
1377  
1378  
1379  
1379  
1380  
1381  
1382  
1383  
1384  
1385  
1386  
1387  
1388  
1388  
1389  
1389  
1390  
1391  
1392  
1393  
1394  
1395  
1396  
1397  
1398  
1398  
1399  
1399  
1400  
1401  
1402  
1403  
1404  
1405  
1406  
1407  
1408  
1409  
1409  
1410  
1411  
1412  
1413  
1414  
1415  
1416  
1417  
1418  
1419  
1419  
1420  
1421  
1422  
1423  
1424  
1425  
1426  
1427  
1428  
1429  
1429  
1430  
1431  
1432  
1433  
1434  
1435  
1436  
1437  
1438  
1439  
1439  
1440  
1441  
1442  
1443  
1444  
1445  
1446  
1447  
1448  
1449  
1449  
1450  
1451  
1452  
1453  
1454  
1455  
1456  
1457  
1458  
1459  
1459  
1460  
1461  
1462  
1463  
1464  
1465  
1466  
1467  
1468  
1469  
1469  
1470  
1471  
1472  
1473  
1474  
1475  
1476  
1477  
1478  
1479  
1479  
1480  
1481  
1482  
1483  
1484  
1485  
1486  
1487  
1488  
1488  
1489  
1489  
1490  
1491  
1492  
1493  
1494  
1495  
1496  
1497  
1498  
1498  
1499  
1499  
1500  
1501  
1502  
1503  
1504  
1505  
1506  
1507  
1508  
1509  
1509  
1510  
1511  
1512  
1513  
1514  
1515  
1516  
1517  
1518  
1519  
1519  
1520  
1521  
1522  
1523  
1524  
1525  
1526  
1527  
1528  
1529  
1529  
1530  
1531  
1532  
1533  
1534  
1535  
1536  
1537  
1538  
1539  
1539  
1540  
1541  
1542  
1543  
1544  
1545  
1546  
1547  
1548  
1549  
1549  
1550  
1551  
1552  
1553  
1554  
1555  
1556  
1557  
1558  
1559  
1559  
1560  
1561  
1562  
1563  
1564  
1565  
1566  
1567  
1568  
1569  
1569  
1570  
1571  
1572  
1573  
1574  
1575  
1576  
1577  
1578  
1579  
1579  
1580  
1581  
1582  
1583  
1584  
1585  
1586  
1587  
1588  
1588  
1589  
1589  
1590  
1591  
1592  
1593  
1594  
1595  
1596  
1597  
1598  
1598  
1599  
1599  
1600  
1601  
1602  
1603  
1604  
1605  
1606  
1607  
1608  
1609  
1609  
1610  
1611  
1612  
1613  
1614  
1615  
1616  
1617  
1618  
1619  
1619  
1620  
1621  
1622  
1623  
1624  
1625  
1626  
1627  
1628  
1629  
1629  
1630  
1631  
1632  
1633  
1634  
1635  
1636  
1637  
1638  
1639  
1639  
1640  
1641  
1642  
1643  
1644  
1645  
1646  
1647  
1648  
1649  
1649  
1650  
1651  
1652  
1653  
1654  
1655  
1656  
1657  
1658  
1659  
1659  
1660  
1661  
1662  
1663  
1664  
1665  
1666  
1667  
1668  
1669  
1669  
1670  
1671  
1672  
1673  
1674  
1675  
1676  
1677  
1678  
1679  
1679  
1680  
1681  
1682  
1683  
1684  
1685  
1686  
1687  
1688  
1688  
1689  
1689  
1690  
1691  
1692  
1693  
1694  
1695  
1696  
1697  
1698  
1698  
1699  
1699  
1700  
1701  
1702  
1703  
1704  
1705  
1706  
1707  
1708  
1709  
1709  
1710  
1711  
1712  
1713  
1714  
1715  
1716  
1717  
1718  
1719  
1719  
1720  
1721  
1722  
1723  
1724  
1725  
1726  
1727  
1728  
1729  
1729  
1730  
1731  
1732  
1733  
1734  
1735  
1736  
1737  
1738  
1739  
1739  
1740  
1741  
1742  
1743  
1744  
1745  
1746  
1747  
1748  
1749  
1749  
1750  
1751  
1752  
1753  
1754  
1755  
1756  
1757  
1758  
1759  
1759  
1760  
1761  
1762  
1763  
1764  
1765  
1766  
1767  
1768  
1769  
1769  
1770  
1771  
1772  
1773  
1774  
1775  
1776  
1777  
1778  
1779  
1779  
1780  
1781  
1782  
1783  
1784  
1785  
1786  
1787  
1788  
1788  
1789  
1789  
1790  
1791  
1792  
1793  
1794  
1795  
1796  
1797  
1798  
1798  
1799  
1799  
1800  
1801  
1802  
1803  
1804  
1805  
1806  
1807  
1808  
1809  
1809  
1810  
1811  
1812  
1813  
1814  
1815  
1816  
1817  
1818  
1819  
1819  
1820  
1821  
1822  
1823  
1824  
1825  
1826  
1827  
1828  
1829  
1829  
1830  
1831  
1832  
1833  
1834  
1835  
1836  
1837  
1838  
1839  
1839  
1840  
1841  
1842  
1843  
1844  
1845  
1846  
1847  
1848  
1849  
1849  
1850  
1851  
1852  
1853  
1854  
1855  
1856  
1857  
1858  
1859  
1859  
1860  
1861  
1862  
1863  
1864  
1865  
1866  
1867  
1868  
1869  
1869  
1870  
1871  
1872